

Datenbanken und Datensicherheit

Musterlösung zu den Übungsaufgaben 12 – 15. Januar 2025

Aufgabe 1: Kryptographie für Gruppen

Eine verschlüsselte Nachricht (z. B. E-Mail) soll gleichzeitig für mehrere Personen lesbar sein.

- (a) Jemand schlägt vor, die Nachricht zu vervielfältigen und jede Kopie mit dem öffentlichen Schlüssel jeweils einer Person zu verschlüsseln. Welche Nachteile hat diese Vorgehensweise?
- (b) Schlagen Sie eine sinnvollere Vorgehensweise vor.

Lösung

- (a) **Jemand schlägt vor, die Nachricht zu vervielfältigen und jede Kopie mit dem öffentlichen Schlüssel jeweils einer Person zu verschlüsseln. Welche Nachteile hat diese Vorgehensweise?**

Eine gesamte Nachricht asymmetrisch zu verschlüsseln, ist viel zu aufwendig und daher ineffizient.

Durch die Vervielfältigung der Nachricht entsteht außerdem das neue Problem, daß nicht mehr garantiert ist, daß alle Empfänger wirklich dieselbe Nachricht bekommen.

- (b) **Schlagen Sie eine sinnvollere Vorgehensweise vor.**

Wesentlich sinnvoller als asymmetrische Verschlüsselung der Nachricht ist eine hybride Verschlüsselung, bei der nur ein Sitzungsschlüssel asymmetrisch verschlüsselt wird.

Durch diese „Parallelschaltung“ der asymmetrischen Verschlüsselung entsteht eine Oder-Verknüpfung der Berechtigungen.

Um zu gewährleisten, daß alle Empfänger wirklich dieselbe Nachricht bekommen, bietet es sich nun an, denselben Sitzungsschlüssel mit jedem öffentlichen Schlüssel einzeln zu verschlüsseln. (Alternativ ließe sich dies auch durch eine Signatur der Nachricht gewährleisten.)